DEPARTMENT OF DEFENSE

Report to Congress

on the

USE OF SMART CARD TECHNOLOGY

IN THE

DEPARTMENT OF DEFENSE

June 1999

DOD SMART CARD PROGRAM REPORT

Executive Summary

This report responds to a requirement by the Strom Thurmund National Defense Authorization Act for fiscal year 1999 (Section 344, Oversight of Development and Implementation of Automated Identification Technology (AIT)). That section required that the Department of Defense (DoD) submit a plan to the congressional defense committees for the use of smart card technology by each Military Department. The Department provided an interim response on April 2, 1999. This represents the final report.

In February 1997, Vice President Gore's National Performance Review and the Government Information Technology Services Board called for the "use of information technology to reengineer the government's business processes and provide public electronic access to the government's services and information." A report published by the federal Electronic Processes Initiatives Committee (EPIC) Card Services Task Force further stated that: "Smart card systems serve as the ideal platform to support the government's business process reengineering for the future."

In keeping with these government reinvention initiatives and paperwork reduction plans, the Department has, over the last several years, investigated the potential for deploying smart card technology. The DoD Multi-Automated Reader Card (MARC) demonstrations in fiscal years 1995 and 1996, and more recent Smart Card Technology Office (SCTO) evaluations, indicate the potential for significant process improvements from the use of smart cards. These indications are that DoD use of smart card technology ultimately may:

- Enable business performance improvement and business process reengineering;
- Increase customer satisfaction and improve quality of life;
- Enhance mission accomplishment;
- Enable movement of data from one legacy system to another;
- Authenticate users for access/security requirements;
- Eliminate redundant data entry;
- Reduce proliferation of single use, non-standard automated cards; and
- Satisfy requirements for updateable information on a portable medium.

In recognition of this potential, a total of $10 million was identified for fiscal years 1998 and 1999 to explore ways for the Department to capitalize upon recent technological advances in smart card technology. In 1997, a Smart Card Senior Steering Group was formed and the Navy was designated as the lead Service for a demonstration in Hawaii. The SCTO was established in October 1997.

A report on smart card implementation and the benefits to be derived is due to the Smart Card Senior Steering Group from the SCTO by September 30, 1999. Demonstrations are ongoing and business case analyses (BCAs) are being prepared in several functional areas with potential plans for wide deployment of smart cards in fiscal years 1999 and 2000 based on the state of maturity of the evolving technology.

This report to the Congress discusses what the Department has accomplished to date, our approach, and the planning required to proceed, predicated on the preliminary results of our findings to date. The Department bases business decisions for employing smart card technology primarily on the results of business case analyses. The current course of action is to continue employing business case analysis techniques as the best way of assessing the most appropriate use of smart card technology. This process is ongoing across the DoD Components (i.e., the Military Departments, Joint Chiefs of Staff and the Combatant Commands, Defense Agencies and DoD Field Activities). Costs can be projected on a very broad scenario and savings can be derived as an order of magnitude. Although the estimated investments and savings are imprecise at this time, a strong management approach continues to be taken to capitalize on the smart card technology, leverage existing investments, and ensure interoperability and cooperation with other government agencies and industry.

Table of Contents

1.0. Background

1.1. Congressional Requirement

This report responds to a requirement set forth in the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (Section 344, Oversight of Development and Implementation of Automated Identification Technology (AIT)). Specifically, the Secretary of Defense was required to submit to the congressional defense committees a plan for the use of smart card technology. The Department of Defense (DoD) previously forwarded an interim response on April 2, 1999.

1.2. Smart Card Defined

The Department adheres to the federal definition of a smart card which comports with the definition in Section 344 of the Act. The federal definition is: "The term 'smart card' means a credit card size card with an integrated circuit chip (ICC), or microprocessor, which meets the International Standards Organization 7816 standard for smart cards. A multi-application smart card can be used for several functions and may employ several technologies, such as bar code, magnetic stripe, etc., in addition to the ICC."

1.3. DoD Contextual Framework

In February 1997, the National Performance Review under the direction of Vice President Al Gore, and the Government Information Technology Services Board published a report titled *Access America: Reengineering Through Information Technology*. The *Access America* report calls for the "use of information technology to reengineer the government's business processes and provide public electronic access to the government's services and information. It is the Administration's goal to use smart card-based systems to improve a wide range of the government's business processes and advance electronic commerce on a government wide basis. Smart card technology offers the government an entrance ramp for the efficient use of the National Information Infrastructure as a federal electronic business highway."

To support the government re-invention initiatives, process streamlining, and paperwork reduction plans, the Department has investigated the potential deployment of smart card technology applications and has initiated demonstration projects as proofs of concept. The Department continually searches for better ways to employ scarce resources in order to meet its operational mission requirements. DoD business streamlining and cost-cutting initiatives have the potential to reduce indirect business costs, which then can be used to meet warfighter mission requirements. However, the Department is faced with a very complex and interdependent business environment that makes successful implementation of streamlining and cost-cutting efforts across the enterprise difficult. The Department fully recognizes this problem, but remains committed to driving down support costs. To that end, the Department has aggressively pursued electronic business/electronic commerce (EB/EC) targets of opportunity throughout the defense infrastructure. The

Department recognizes that EB/EC concepts and technologies, such as smart cards, are the leveraging tools needed to accomplish requisite infrastructure savings DoD-wide.

The Deputy Secretary of Defense issued a series of directives that support and amplify the Defense Reform Initiative (DRI) Report. On May 20, 1998, the Deputy Secretary signed DRI Directive #43 – "Defense-wide Electronic Commerce," which established the Joint Electronic Commerce Program under the policy direction of the DoD Chief Information Officer (CIO). The assignment of EB/EC responsibilities to the DoD CIO enables EB/EC to complement business process changes throughout the functional areas of the Department. The CIO published an EB/EC Guidance and Policy Memorandum that sets forth initial policy direction, roles, and responsibilities. Further, the CIO recently released the "DoD EB/EC Strategic Plan," which sets forth the Department EB/EC vision, goals, objectives and strategies, to include smart cards. Ongoing actions include the publication of a DoD directive on the EB/EC program and the integration of EB/EC into the Department's overall "Information Technology Management Strategic Plan."

2.0. Current DoD Smart Card Program

2.1. DoD CIO Leadership

Smart card-related technologies give the Department a set of robust tools to use in reengineering business processes within the context of the overall DoD Joint EB/EC Program. The smart card program and associated plans and initiatives are not an independent program but an integral piece of the overall DoD EB/EC program. As such, smart card initiatives adhere to the overall DoD management philosophy of centralized management and decentralized execution. Therefore, the DoD CIO, other Principal Staff Assistants in the Office of the Secretary of Defense (OSD), and the Joint Staff set forth the high-level strategies, plans, policies and business processes, and conduct oversight reviews and participate fully in the resource allocation process. Development and operational execution is performed at the DoD Component level. Management and program integration are accomplished by a special EB/EC element of the DoD CIO Council, named the CIO Working Council.

2.2. Smart Card Senior Steering Group (SCSSG)

In recognition of the potential process and resource benefits obtained through effective application of smart card technology, the Department chartered a senior level oversight group: the SCSSG. The SCSSG provides policy guidance and reviews functional aspects of Smart Card Technology Office (SCTO) work. The membership of the SCSSG consists of the following:

- Principal Deputy Under Secretary of Defense (Comptroller) (Chair)
- Department of Defense Deputy Chief Information Officer (CIO)
- Director, Force Structure, Resources and Assessment, The Joint Staff (JCS)
- Deputy Under Secretary of Defense, Program Integration

- Director of Defense Procurement
- Director, Program Analysis and Evaluation

2.3. Smart Card Technology Office (SCTO)

To coordinate and provide leadership for the required smart card operational initiatives, the Department established the SCTO in October 1997 as an element of the Defense Manpower Data Center (DMDC). At the departmental level, many issues such as the core applications, costs of infrastructure, replacement of the current military identification (ID) card, methods and costs of card issuance and management are being addressed. The SCTO was formed to address these questions, define the necessary requirements, identify and resolve policy issues and review technology recommendations. The SCTO is staffed in part with representatives from the Army, Navy, and Air Force to help foster coordination and interoperability among and across the Services. Its charter states that "the mission of the SCTO is to conduct an evaluation of smart card technology within the Department of Defense (DoD) to include an on-going demonstration in Hawaii." Under the mission, the charter further specifies the following six tasks for the SCTO:

- Establish a body of expertise on the application of smart card technology within DoD;
- Develop a consensus on the implementation of smart card technology within the DoD;
- Make a recommendation on whether or not the smart card should be adopted as the universal ID card;
- Assess cost and impact of implementing smart card technology to include infrastructure and associated systems;
- Coordinate demonstration projects to ensure appropriate data are available for evaluation; and
- Determine a DoD configuration management strategy that would ensure continuity and interoperability across applications and functions.

The SCSSG has authorized the establishment of working groups to gain functional expertise and gather requirements. Functional Working Groups have been established for Theater Medical, Transportation, the Military Academies, Financial, and Security. Membership for each working group is drawn from the DoD Components.

All smart card prototype demonstrations initiated after October 1997 in the Department are conducted with the approval of the SCTO. The information, applications and lessons learned are shared. The Department funds the demonstration on Oahu, mentioned in the SCTO Charter, while each Military Department funds other demonstrations.

The SCTO is scheduled to “sunset” on September 30, 1999. The future placement of the smart card day-to-day management function is undergoing analysis. The OSD staff, led by the DoD CIO, is evaluating future program office roles, responsibilities, and

functionalities. The future mission will be determined, placement criteria will be formulated, and an organizational placement will be proposed through the CIO Council and the SCSSG for approval by the Deputy Secretary.

2.4. Smart Cards and Public Key Infrastructure (PKI)

The Deputy Secretary recently issued PKI implementation policy guidance that could lead to significant utilization of smart card technology. That guidance is summarized in this section.

Achieving information superiority in a highly interconnected, shared-risk environment requires that DoD's Information Assurance (IA) capabilities address the pervasiveness of information as a vital aspect of business operations. The technical strategy that underlies DoD IA is "Defense-in-Depth," which provides for layers of defense to achieve our security objectives. To ensure consistent, proper usage of different information assurance levels across the Department, the assurance levels of PKI certificates issued and used for particular applications are in accordance with the U.S. DoD X.509 Certificate Policy. Under the current DoD PKI policy, there are five classes of assurance[1]. Smart cards may be used in achieving Class 3 (medium level assurance) and Class 4 (high level assurance) certifications. The use of smart cards as hardware tokens to store class 4 certificates affords protection of unclassified, mission critical information over unencrypted networks. Category 1[2] mission critical systems, operating on unencrypted networks and employing public key technology, immediately must begin the migration to Class 4 certificates and tokens (e.g., smart cards, PC cards, or universal serial bus cards) and should achieve full implementation by June 2000.

2.5. Smart Card Interoperability

Interoperability refers to the cooperative processing of an application by distinct software, hardware/firmware, and various generations of cards and terminals, operating procedures, or administrative procedures. The Department is striving to establish an interoperable environment in which there is sufficient flexibility to accommodate cards from multiple issuers and provide access to multiple services. In this environment, there will be flexibility at all levels of service delivery, investments by consumers and service providers are protected, and customers have vendor-independent access to services. The Department is participating in supporting technical interoperability standards.

While technical standards ensure "physical" compatibility, operating rules provide the management and administrative framework to ensure that transactions are properly

---

[1] Deputy Secretary of Defense Memorandum, May 6, 1999, Subject Department of Defense (DoD) Public Key Infrastructure (PKI)

[2] Defined by the Clinger-Cohen Act as National Security Systems (intelligence activities; cryptographic activities related to national security; command and control of military forces; integral to a weapon or weapons system; and systems critical to direct fulfillment of military or intelligence missions).

handled. Within an open system, operating rules constitute the components of binding business arrangements among the system participants and stakeholders. The Department is participating in the General Service Administration's (GSA's) Smart Access Common ID Card pilot program that will begin the intra-agency establishment of smart card operating rules.

In the absence of the full range of standards needed to achieve seamless interoperability, it may be possible to achieve acceptable levels of interoperability among competing, multifunctional card programs. In the longer term, it increasingly will become possible to achieve more extensive interoperability. While attaining interoperability at the card level currently is a challenge, accomplishing interoperability at the application level is even more complex. The emerging PKI, however, may become the mechanism for achieving government-wide interoperability at a higher application level. To address the complexities of achieving interoperability across incompatible physical and computer and network access control systems, one theoretically could use the emerging PKI as a mechanism to assist in verifying the identity of the cardholder and the validity of the smart card. This would potentially lead to a DoD-wide common access card that we expect to begin pilot testing this summer.

3.0. Business Process Improvement

The SCTO is chartered to evaluate the current state of smart card use in the Department. As previously stated, decisions to apply smart card technology to DoD's business processes are being made following the conduct and review of BCAs. Where process redesign, improvements and technology implementation result in cost savings and a favorable return on investment, the Department will invest in smart card technology. Explicit process baselining, data collection and analysis are conducted prior to making a technology investment decision. A business based approach coupled with proven management decision tools (such as the BCA) enable the SCTO to forward concrete recommendations to decision makers.

The implementation of smart card technology focuses on the key performance areas of cost savings, mission enhancement, and quality of life. It is important to introduce the technology only where reinforced by business principles.

The methodology used to conduct the BCAs for smart card performance throughout the various demonstrations incorporates three distinct project phases. The first phase entails the development of a comprehensive data collection plan to gather representative information. Collection of the data comprises the second phase, and the last phase is a detailed analysis of the collected data. Several analytical tools are used. The BCA is conducted to analyze the potential benefits provided by the use of smart card technology vice the existing business process.

4.0. Smart Card Program Demonstration Initiatives (Selected)

The OSD and the Military Departments have made substantial investments in smart card technology. The Department, with the SCTO as its agent, uses an approach that supports

the goal of complete interoperability within the Department, with other federal agencies and with the private sector. In concert with meeting the goal of interoperability, the Department has included as an objective the requirement to leverage existing infrastructure to the best extent possible. In support of this, many demonstrations are considered prototypes in nature and are intended to provide proof of concept and macro cuts at potential costs and benefits. Potential benefits from the smart card demonstrations are identified in Table 1.

4.1. Joint Applications and Demonstrations

Oahu Demonstrations. The SCTO has sponsored smart card demonstrations featuring applications with joint interoperability on Oahu, Hawaii since FY 1998. The Military Departments, DMDC, and the Defense Finance and Accounting Service (DFAS) are active participants in the development and implementation of smart card technology on Oahu. To date, food service, armory, vehicle pass and tag, facility access, and warrior readiness applications have been developed and implemented at one or more Army, Navy, Marine Corps, or Air Force facilities on Oahu. Beginning this year, re-engineering efforts are underway for the Personnel Support Activity Detachment (PSD), Pearl Harbor, funded by the Navy. The use of smart card technology is expected to achieve efficiencies in the personnel and pay functions conducted at the PSD and at the Personnel Support Activity level.

DEERS/RAPIDS Demonstrations. Examples of leveraging existing infrastructure are evidenced in several initiatives. Two of these are the Smart Card/Real-Time Automated Personnel Identification System (RAPIDS) integration demonstration and the use of Defense Eligibility and Enrollment Reporting System (DEERS) to store back-up data. The smart card/RAPIDS demonstration is being conducted at the Navy PSD Pearl Harbor Naval Base. RAPIDS software, which generates the standard military ID card, was modified to incorporate smart card software issuance and peripheral devices. The same platform and source data that generate military ID cards now can generate smart cards. The smart card/RAPIDS demonstration, which began in February 1999, has been successful. Cost savings from using existing infrastructure, productivity benefits from improved customer throughput (more workstations available for more functions), and improved staffing from cross-trained workers are just a few derived benefits from this demonstration. Leveraging the existing RAPIDS investment for card issuance is a potential cost avoidance of approximately several million dollars in hardware alone.

DEERS is the existing database system that stores data for all DoD personnel (military members, civilian employees, dependents, military retirees, and annuitants). The architecture of DEERS allows the addition of functionality without major re-work. By leveraging existing database structures, capacity, and expertise, a mirror image of an individual's smart card data could be stored in DEERS. This capacity, with minimal investment, will allow restoration of data in the case of a lost or damaged smart card. This avoids the addition of a management structure and hardware investment.

The leveraging of previous investments is a consistent theme. Software is used by all DoD Components and designed to maintain Component identity and interface to

component specific systems. Card and equipment upgrades should be both backward and forward compatible to capitalize on existing investments.

Cobra Gold 98. Cobra Gold is the name of a large, bilateral exercise between the United States and Thailand designed to ensure regional peace throughout the geographic area covered by the U.S. Pacific Command. The U.S. Marine Corps is the lead service. The exercise that was evaluated was conducted May 19-June 1, 1998, and served as a crucible for piloting several smart card applications. This exercise included joint-combined land and air operations, combined naval operations, amphibious operations, and special operations. Participating U.S. Forces totaled approximately 10,600 and included elements of U.S. Marine Forces, Pacific; U.S. Army Pacific; U.S. Pacific Air Forces; U.S. Pacific Fleet; Special Operations Command, Pacific; Air Mobility Command; Military Sealift Command; and Reserve Component (RC) units of the Army, Navy, Air Force and Marine Corps.

Since movement of forces and equipment in and out of Thailand during Cobra Gold 98 was such huge undertaking, smart card technology was applied to aircraft manifesting of personnel and materiel. The results of that effort were most encouraging and may be found in Section 5.0

4.2. Military Department Applications and Plans

4.2.1. Department of the Army

The Army has several smart card demonstrations in the continental United States (CONUS) and outside CONUS. Demonstrations launched or participated in to date include the 2nd Armored Cavalry Regiment multiple application smart card demonstration; the DFAS stored value card (SVC); and the Forces Command mobilization and readiness smart card initiative. All of these pilots have shown that smart cards enhance warfighter capabilities and further EC development across the Department.

2nd Armored Cavalry Regiment. The 2nd Armored Cavalry Regiment (ACR) tested a multiple application smart card during that unit's redeployment from Bosnia to Fort Polk, Louisiana. The soldiers of the 2nd ACR, home-based at Fort Polk and assigned to the Bosnia mission, used smart card for manifesting during their redeployment to CONUS. The unit was issued cards as part of a deployment exercise during the summer of 1998. The primary purpose of the Bosnia demonstration was to have "in-transit visibility" (ITV) of soldiers moving from port of debarkation to port of embarkation. Smart cards provided visibility of every soldier in the deployment. It took only one day to initialize 2,400 smart cards and six seconds to manifest a soldier; visibility of the soldier by unit line number and mission number via the Global Transportation Network was achieved in less than one hour. This demonstration supports the operational and administrative objectives mission and more importantly showed firm support for warfighter capability. Activities that previously took several days in Saudi Arabia during Operation Desert Storm were reduced to a few hours in Bosnia.

25th Infantry Division (Hawaii). For the past two years, the 25th Infantry Division has been the Army's primary unit for piloting many smart card applications. The 25th Infantry Division has piloted applications such as manifesting and personnel readiness. These functions, which previously took an entire day to accomplish for 2000 soldiers, now take four hours. Processing soldiers for rapid deployment using the old system meant reserving a gymnasium or the largest building on post a week in advance and setting up 12 stations to process various aspects of the soldiers' record. Now, using the smart card, 2,000 soldiers are processed at only applicable stations, spending no more than 30 minutes at each station. The smart card is proving to be beneficial when it comes to personnel readiness processing.

Army Basic Training. The Department of the Army is testing an SVC application at five Army basic training installations. This test is being conducted in partnership with the Department of the Treasury's Financial Management Service, the DFAS, and the Army and Air Force Exchange Service (AAFES). Over 150,000 trainees have been issued SVCs, which have been used for over 1 million transactions valued at over $28 million. According to the Department of the Treasury, the Army's SVC program is one of the largest and most successful SVC implementation in the United States. The SVCs replace cash and check payments and paper voucher system of their initial advance pay. Trainees use the funds on the SVC to pay for personal items such as toiletries and haircuts during their eight weeks of basic training. At the end of basic training, the trainee can "cash out" any balance remaining on the smart card at an on-post financial institution. If the soldier takes no action, the card expires and any unused portion is credited to his or her military pay or checking account. Three security applications have been tested. Fort Knox used a personal identification number (PIN); Fort Sill used biometrics (finger print); and Forts Leonard Wood, Benning and Jackson used no PIN. All five demonstrations showed that the Department of the Army will reduce administration time for processing trainees, increase training time, decrease issuing checks, reduce cash operations, and enhance barracks security.

Additionally, the Army has gained experience with smart cards for supporting financial transactions in peace and during military operations. From the beginning, SVC technology has demonstrated its value. Exchange Service cashiers are able to process purchases by trainees who present smart cards usually in 30-40 seconds or less, which is much faster than those paying with cash or checks. Unlike cash, SVCs can be replaced when lost or stolen. On-base merchant activities electronically deposit their revenues at the end of each day through a toll-free number via the Automated Clearing House. There is less cash in the hands of trainees and the installations (over $28 million less since 1997). An advantage to the individual trainee is the elimination of a personal cost (estimated at $115,000) to purchase money orders or travelers check. Most importantly, SVCs have been well received by the training cadres and the trainees.

The Fort Sill SVC with fingerprint biometrics was honored at the 1998 CardTech/ SecurTech Conference as the recipient of the Larry Linden Innovative Security Applications Award. The award recognizes achievements in the fields of advanced card technology and biometrics.

The smart card has demonstrated significant benefits to soldiers and to the Army.

Forces Command. The U.S. Army Forces Command (FORSCOM) employed smart cards in OPERATION CALL FORWARD 97, which was conducted in Puerto Rico. FORSCOM used a software application (Mobilization Level Application Software (MOBLAS)) to compress soldier data in excess of 8K and exported those data to smart cards. It was then decompressed and uploaded to a separate computer. The pilot test evaluated the ability to configure personnel records onto portable electronic files, easily managed and updateable. This demonstration proved value added in records management oversight and security of personnel records for FORSCOM.

As the mobilizer and deployer for the Army, FORSCOM selected two Reserve Component RC units for further testing. During FOAL EAGLE 98, held in Korea, soldiers also were issued smart cards. Soldiers used smart cards for ITV manifesting through the Global Transportation Network. The test validated the use of the smart card by the RC during actual mobilization and deployment.

FORSCOM also has identified units of the III Corps, 10th Mountain Division, 4th Infantry Division, and the Texas Army National Guard to participate in the use of the DoD smart card during their deployments to Tuzla, Bosnia. Additionally, FORSCOM will process Army National Guard units to SWA utilizing the DoD smart card. FORSCOM's efforts have shown that data from units of more than one Component can be applied to a smart card with significant improvements to the transition of RC to the Active Component systems. During exercise CALL FORWARD 99, a Navy interoperability demonstration is scheduled to be conducted. The demonstration will enhance FORSCOM's ability to support Joint Operations during soldier readiness processing and standardize the multi-service business process. Significant to FORSCOM's initiative is linking a centralized database to the information stored on smart cards and automating soldier readiness processing.

The Department of the Army smart card demonstrations have shown that not only can the military apply civilian applications for military use but that use of this emerging technology greatly enhances warfighting capabilities.

Personal Information Carrier. As directed by the Office of the Assistant Secretary of Defense (Health Affairs) (OASD (HA)), the Army Medical Department is participating in the tri-service medical Personnel Information Carrier (PIC) Project. The purpose of the PIC project is to create a cradle-to-grave electronic health record. The OASD (HA) is meeting this requirement in 3 phases.

Phase 1 is a fixed facility, hospital-based electronic patient record called Composite Health Care II. Phase 2 is a theater based electronic patient record, which is a subset of the Phase 1 fixed facility based record and consists of critical patient encounters. Phase 1 requires large amounts of communications bandwidth 24 hours a day 365 days a year. Phase 2 requires a reduced amount of bandwidth. Phase 3 is for those areas in theater where communications bandwidth is non-existent, unreliable or prioritized for non-medical uses (i.e., combat operations). These areas require a small portable electronic

storage device. This is the Medical Personnel Information Carrier (PIC). When a soldier receives treatment at a Battalion Aide Station or Forward Support Medical Company, the soldier's treatment is recorded on a laptop computer. The laptop computer stores the medical record on its hard drive and on the PIC. The data transfers electronically to the theater electronic patient record from the laptop computer when communications are available. Soldiers carry their PICs with a copy of their treatment data. If they are evacuated or receive follow-on treatment, the receiving medical facility/care provider can insert the PIC into a computer and read their treatment record.

Requirements for the PIC have been defined by the Theater Medical Information Program which falls under the preview of the Joint Requirements Oversight Council. Those requirements include 119 patient demographic and medical data criteria, data on 5 or more patient treatment encounters, a read/write capability, compatibility with the fixed facility electronic patient record, structured patient diagnosis and treatment, and free text entry. Proof-of-concept tests are being planned for the fall of 1999. Operational testing and evaluation is planned in the year 2000.

4.2.2. Department of the Navy

4.2.2.1. Navy

The Navy's strategy to deploy smart cards within the Service began by issuing smart cards to service members as they entered the Navy through the Recruit Training Center (RTC) Great Lakes, Illinois. The Navy's strategy is based on indoctrinating those personnel during their initial training to the uses of smart card technology. The next entry point for smart cards into the Navy was through training commands such as the Service School Command (SSC) Great Lakes; Fleet Combat Training Center (FCTC) Dam Neck, Virginia; and Naval Air Station (NAS) Pensacola, Florida. The final step of smart card deployment within the Navy is driven by the FY 1999 Defense Authorization Act requirement to outfit designated shipboard personnel with smart cards. From that requirement, the Navy has developed a plan to deploy smart card technology throughout the fleet.

RTC Great Lakes. Beginning in late June 1998, all new recruits processed through RTC Great Lakes have been issued a smart card for use with food service, medical, dental, and stored value applications. The food service, medical and dental applications have resulted in reductions in data entry, paper handling, and audit requirements while increasing the accuracy of the data collected. The stored value application, although using a system different from that employed by the Army and Air Force, has had similar results in eliminating cash handling and audit requirements and providing the recruits with a secure, auditable system for the recruit's initial advanced pay. In addition, a student visibility application currently is being used to record each student's arrival at his or her classroom and provide a near real-time accounting of student attendance. Taken to its full vision, this application will include smart card readers at medical and dental clinics, galleys, and dormitories as well as those in classrooms tied together on a local area network. This system will enable real-time visibility over the location of personnel

and reduce the time spent each day by personnel in the Student Control Office to account for the entire student population.

NAS Pensacola. Food service and morale, welfare and recreation applications are in operation at NAS Pensacola. Plans now are complete to install and use the medical and dental applications. A plan also has been developed to use smart cards to replace a paper-based system that controls students' after-hours liberty from their dormitories. The current system is labor intensive to operate and cannot provide an accurate picture of student arrivals and departures. Smart card use will eliminate work and provide a true accounting of student location.

FCTC Dam Neck. At FCTC Dam Neck, plans for food service, medical, dental, and access control applications are complete. The access control application will interface with the building access control system scheduled to be installed and will use two types of smart cards – contactless cards for permanent staff and contact cards for students. This system will eliminate the use of single-use identification badges, allow classroom access to be tightly controlled, and record and time-stamp each student's movements within the school building.

USS Yorktown. The Navy's first cash-less ship, the USS Yorktown, was outfitted with the SmartCity Stored Value system in November 1996. The cruiser is a pilot in the U.S. Navy's Smart Ship Project that uses innovative technology to reduce staff, increase safety and improve life aboard ship. With a stored value limit of up to $200, Sailors use their "electronic purse" to buy anything from snack foods and drinks to t-shirts and supplies. Although there still are some areas using cash, the card is used for many onboard transactions, from the ship's store to the post office, and at all vending machines. Smart cards have increased productivity on board the ship by reducing the number of personnel needed to collect and account for cash for onboard purchases. Since November 1996, the USS Yorktown has recorded over 500,000 transactions. It is recognized as one of the most successful stored value implementations ever, with a workload reduction of 320 workhours/month.

Other Afloat Activities. As directed in the FY 1999 Defense Authorization Act, the Navy is embarking on smart card shipboard installations. Nine applications, ranging from stored value (electronic purse) to quarterdeck control, are planned to complete a shipboard smart card application suite. To meet the requirements of the congressional mandate, the Navy has planned smart card installations on two Carrier Battle Groups and Amphibious Readiness Groups in FY 1999 and has developed a plan to complete the installation throughout the rest of the fleet. Furthermore, shore installations located at Fleet concentration areas also will be targeted for smart card use.

4.2.2.2. U.S. Marine Corps

The U.S. Marine Corps is planning smart card demonstrations in FY 1999 at the Marine Corps Recruit Depot Parris Island, South Carolina (MCRD PISC) and the Marine Corps Air Station (MCAS) New River, North Carolina. The MCRD PISC demonstration, in conjunction with the Navy Smart Card Office and the Department of the Treasury, will

issue a temporary smart card to recruits in a "closed" environment. Initial applications scheduled for use at MCRD PISC are stored value and manifesting/mustering. The MCAS New River demonstration, in partnership with the Navy Smart Card Office, will issue smart cards to permanent personnel. Initial applications planned for MCAS New River are medical, dental, food service, and manifesting/mustering.

4.2.3. Department of the Air Force

4.2.3.1. The Air Force Automatic Identification Technology Program Management Office (AF AIT PMO) at Air Force Materiel Command, Wright-Patterson AFB, Ohio is the lead technical agent for smart cards. The Deputy Director, Global Combat Support System, is the lead proponent of smart cards in the Air Force and is the senior representative to the DoD SCTO.

4.2.3.2. Two smart card applications have been adopted by the Air Force:

a. The Supply Asset Tracking System (SATS) is a front-end processor application to the Standard Base Supply System that tracks all assets in base supply in a real time mode. Smart cards are being used by SATS at Shaw Air Force Base (AFB), South Carolina; Eglin AFB, Florida; Aviano Air Base, Italy; and Ramstein Air Base, Germany for electronic authentication and authorization of the cardholders to receive assets. The use of the smart card for electronic confirmation reduces the amount of paper documentation previously required in the delivery process at the base supply level. A labor intensive and error prone process was greatly improved via the use of this technology.

b. SVCs loaded with initial pay are being issued to all Air Force recruits arriving for training at Lackland AFB, Texas. The concept was demonstrated for one year beginning in June1998 and was a cooperative effort between the Air Force, Department of the Treasury, DFAS, and AAFES using the VISA Cash card. The recruits use their SVCs to make purchases at the base exchange, purchase haircuts and money orders, pay for use of laundry/dry cleaners and phone centers, and make donations at chaplain-conducted religious services. Additional point-of-sale locations are being identified. Although the one-year demonstration identified benefits (reduction in cash handling tasks and data entry workload, reduced cash holding requirements, and an increase in the security of the recruit's funds), there are added costs to purchase cards. Labor savings may be minimal due to systems administration requirements.

4.2.3.3. The Air Expeditionary Force Battlelab (AEFB), Mountain Home AFB, Idaho in conjunction with AF AIT PMO, is conducting a proof of concept demonstration to integrate smart cards into AF readiness process. The goal for the initial concept of operations is to use smart card technology to demonstrate the AEFB Deployment Personnel Accountability and Readiness Tool initiative. The basic premise of the initiative is to provide accurate and timely information to unit commanders and deployment managers on their unit's state of readiness. This, in turn, reduces the support structure needed to deploy personnel. This demonstration will interface with existing Air Force systems that contribute to personnel readiness. The demonstration and business case analysis will be performed with the support of the16th Special Operations Wing at

Hurlburt AFB, Florida and the 366th Air Expeditionary Wing at Mountain Home AFB, Idaho. By leveraging the work of DoD SCTO's Oahu project, this concept will provide a significant profile for the Air Force, to include an Air Base Wing, a Special Operations Wing, an Air Expeditionary Wing, and a Reserve Fighter Wing at Fort Sill, Oklahoma.

4.2.3.4. The United States Air Force Academy (USAFA) was chosen by the AF AIT PMO as a smart card demonstration site due to its "closed environment." The Falcon Card is issued to all USAFA cadets (approximately 4,200) with the intent that a single card eventually will be used for multiple applications. Currently, the only function being used is an electronic purse. Cadets load funds on their cards' electronic purse and use the card for small purchases (laundromats, snacks, and library copiers). Additional point of sale locations will be added for vending, entertainment (tickets and tours), and outdoor recreation. Loading cadet pay on the smart card's second electronic purse is being considered. The use of the electronic purse reduces cash handling by USAFA employees and reduces the amount of cash carried by a cadet. The functional areas being evaluated are medical, access control, manifesting, inventory control, food services, physical and aerobic fitness test results and training qualifications. Multiple applications on a single card provide the ability to automate and streamline various functions and offer the potential for additional savings.

5.0. Costs and Benefits

Most of the smart card demonstrations in the Department have been limited to (and prototypically are intended to provide) proofs of concept. Although there is evidence that there will be some cost savings in the implementation of smart cards, those savings are insufficient to pay for smart cards, either during implementation or maintenance. It also appears unlikely that smart card use will result in any reduced staffing. However, there are significant benefits in the areas of mission enhancement and quality of life. It is premature for the Department to project specific costs and benefits until these prototypes are completed and evaluations of costs, savings and benefits are determined by BCAs. The BCAs are expected to provide time for further analysis to ensure that there are no substantive "hidden systems administration costs". This information, however, is crucial to decision making and each demonstration is required to document this information in accordance with existing Department CIO and financial policies.

Smart card technology use in the Cobra Gold '98 exercise provided substantial benefits. The key finding from that exercise is that reduced manpower is required to manifest an airplane within the mechanical turnaround time of the aircraft, thus reducing the need for infrastructure at the airhead. Operational capability was improved through accurate and timely data to warfighting commanders in theater and visibility of the personnel to those commanders via the Global Transportation Network. Additionally, quality of life for participating Service members was improved because of the decreased time that they were exposed to extreme temperatures and reduced wait time.

The use of smart cards by the Army, Navy and Air Force in lieu of cash, checks or chits, vouchers, and money order processes for initial advances of pay at initial entry (basic training) stations offers early indications that savings will result. An initial evaluation

shows reduced paper and cash handling requirements and provided more security for each Service member's funds. Table 1 describes potential benefits from each of the applications discussed above.

Table 1

	Application	Potential Benefits
Tactical	Warrior Readiness	• Reduced Assessment Time. • Less time to determine individual unit deployability status; results in faster unit deployments.
	Manifesting	• Reduced manifest time. • Eliminated data entry errors. • Increased accuracy of personnel tracking through the process.
Non-Tactical	Access Control	• Positive accounting of personnel. • Controlled access to sensitive spaces.
	Medical	• Reduced data entry/paper handling. • Reduced time to create medical records, medical force structure savings and change in health care practices for warfighters. • Increased accuracy of information.
	Dental	• Reduced data entry. • Technicians available to provide treatment vs. data entry/paper handling.
	Food Service	• Reduced cash holdings and daily audits. • Simplified and increased accuracy of headcount. • Reduced the number and complexity of forms for cash collection. • Complete and accessible audit trails.
	Personnel Transactions	• Reduced processing time. • Eliminated data entry errors. • Capability to rapidly produce automated Soldier Readiness Processing. Reports by unit commander.
	Stored Value	• Reduced cash handling and audits. • Reduced potential for crime.
	Rifle Range	• Reduced workload required to complete and document qualifications.
	Equipment Issuance	• Positive record of equipment issuance. • Prioritized preventive maintenance; reduced loss potential.

6.0. Proposed Future Smart Card Configuration Management Plan

6.1. Need for the Plan

The DoD approach to the application of smart card technologies still is being developed. There have been several relatively small-scale targeted initiatives and most of them have been highly successful. But, until the establishment of the SCTO and the migration of the DoD smart card management to a major DoD program, there were few large-scale,

cross-service or joint smart card initiatives. To mature the DoD Smart Card Program, the Department is developing an overall configuration management plan that will provide for orderly growth and efficient management of smart cards across the Department. This Plan might permit the DoD program to integrate with other federal smart card initiatives (e.g., GSA's SmartGov/Smart Card Technology, Office of Smart Card Initiatives).

6.2. Process to produce the Plan

The DoD CIO is responsible to oversee the effective and efficient use of all DoD Information Technology (IT). The CIO provides IT policy and oversight, which also is applicable to smart card technologies and applications. The DoD CIO also serves as the functional proponent for EB/EC and will oversee the infusion of smart card technologies into DoD systems. The DoD CIO will develop and oversee a coordinated process that will generate a DoD Smart Card Configuration Management Plan, to include appropriate functional inputs. The SCTO is setting the operational structure that drives the framework for the DoD Smart Card Plan. Consideration is being given to incorporating a DoD Smart Card Configuration Management Plan as an Annex in the upcoming revision to the "DoD Information Technology Management Strategic Plan."

In formulating the Smart Card Configuration Management Plan, the Department will consider the wide variety of smart card applications that range from credit/debit card-like financial tools, to medical personnel identification carriers (PIC), to identification and access cards, and many more. Accordingly, the DoD-wide management of smart cards must identify a sufficiently broad approach and must be coordinated with those DoD Components that have made significant investments in the smart card technologies and applications.

The process to produce an overarching DoD Smart Card Configuration Management Plan will involve the participation of a cross-section of the principal users of the technologies. It will apply lessons learned from the several ongoing small-scale demonstrations and Component-unique initiatives. As it becomes available, supporting information is gleaned from the ongoing demonstrations and initiatives for use in preparing the Plan.

7.0. Summary

The Department anticipates the implementation of multi-application smart cards across functions and DoD Components. Additionally we recognize the high potential represented by smart card technologies. Currently, this potential appears best suited to specific applications that must be brought under centralized configuration control in order to enable global or enterprise applications and business process solutions. At the same time, the Department recognizes that this is a rapidly changing technology. In order to obtain the required degree of interoperability among DoD systems, the Department must move towards this technology in a rational manner in order to obtain the best benefits. The Department, therefore, is working with the smart card industry to set DoD standards that are compatible with industry standards in order to minimize cost and increase competition yet meet the Department's needs for a multi-application, interoperable smart card.

In recognition of this environment, the Department is managing risk by instituting prototype demonstrations. Numerous smart card demonstrations and pilots have been initiated with many approaching the evaluation stage. Some of these demonstrations have been conducted in conjunction with other federal agencies. Results to date indicate that smart card technology, especially when applied with process redesign, provides a positive return of investment as well as enhanced mission readiness and improved quality of life for the warfighter and combat support communities.